Docket No. 216642US8/btm

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Shoji FUKUTOMI, et al.

GAU: 2681

SERIAL NO: 09/996,923

EXAMINER:

FILED: November 30, 2001

FOR: SESSION SHARED KEY SHARING METHOD, WIRELESS TERMINAL AUTHENTICATION METHOD, WIRELESS TERMINAL AND BASE STATION DEVICE

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of **35 U.S.C. §120**.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §119(e)**.
- ■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2000-381042	December 14, 2000
JAPAN	2001-139288	May 9, 2001

Certified copies of the corresponding Convention Application(s)

- ■ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number . Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

  (B) Application Serial No.(s)
  - ☐ are submitted herewith
  - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Registration No. 40,073

Paul A. Sacher
Registration No. 43,418

22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

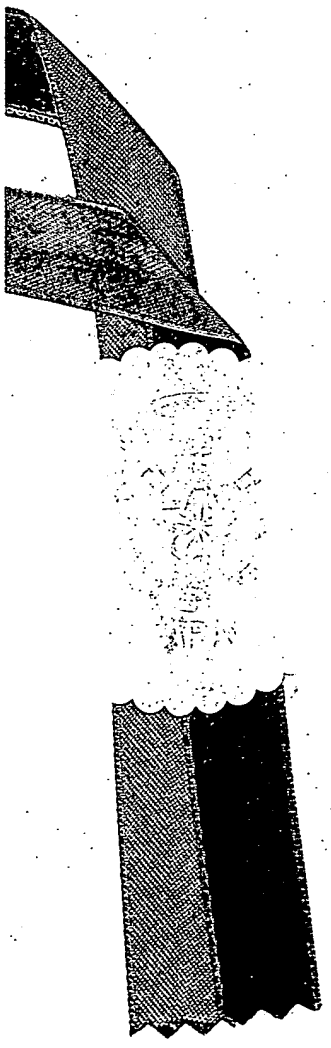
This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月１４日

出願番号
Application Number: 特願２０００－３８１０４２

[ST.10/C]: [ＪＰ２０００－３８１０４２]

出願人
Applicant(s): 古河電気工業株式会社



２００２年 １月２２日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特２００２－３０００３４６

【書類名】　特許願

【整理番号】　A00571

【提出日】　平成12年12月14日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/00

H04B 7/00

【発明者】

【住所又は居所】　東京都千代田区丸の内２丁目６番１号　古河電気工業株式会社内

【氏名】　福富　昌司

【発明者】

【住所又は居所】　東京都目黒区大岡山２－１２－１　東京工業大学内

【氏名】　太田　昌孝

【特許出願人】

【識別番号】　000005290

【氏名又は名称】　古河電気工業株式会社

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セッション共有鍵共有方法、無線端末認証方法、無線端末および基地局装置

【特許請求の範囲】

【請求項１】　パケットを送受信する無線端末と該パケットを中継する基地局装置とが無線を介して通信する場合に、秘匿用および／または認証用のセッション共有鍵を前記無線端末側および前記基地局装置側に共有させるセッション共有鍵共有方法であって、

前記無線端末と前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から前記基地局装置側に対して送信されるパケットに前記セッション共有鍵の生成に用いる第１の情報を挿入する第１挿入工程と、

前記プロトコルに基づいて前記基地局装置側から前記無線端末側に対して送信されるパケットに、前記セッション共有鍵の生成に用いる第２の情報を挿入する第２挿入工程と、

前記基地局装置側で、前記第１挿入工程で挿入された前記第１の情報に基づいて前記セッション共有鍵を生成する第１生成工程と、

前記無線端末側で、前記第２挿入工程で挿入された前記第２の情報に基づいて前記セッション共有鍵を生成する第２生成工程と、

を含むことを特徴とするセッション共有鍵共有方法。

【請求項２】　前記プロトコルは、ネットワーク層アドレスとＭＡＣアドレスとを対応させるプロトコルであることを特徴とする請求項１に記載のセッション共有鍵共有方法。

【請求項３】　前記プロトコルは、ＡＲＰであることを特徴とする請求項１に記載のセッション共有鍵共有方法。

【請求項４】　前記プロトコルは、ネットワーク層アドレスを前記無線端末に割り当てるプロトコルであることを特徴とする請求項１に記載のセッション共有鍵共有方法。

【請求項５】　前記プロトコルは、ＤＨＣＰであることを特徴とする請求項１に記載のセッション共有鍵共有方法。

【請求項６】　パケットを送受信する無線端末と該パケットを中継する基地局装置とが無線を介して通信する場合に、前記基地局装置側で前記無線端末を認証する無線端末認証方法であって、

前記認証に用いるセッション共有鍵の生成用の第１の情報を秘密鍵によって暗号化する暗号化工程と、

前記無線端末と前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から前記基地局装置側に対して送信されるパケットに、前記暗号化工程で暗号化された前記第１の情報を挿入する第１挿入工程と、

前記基地局装置側で、前記第１挿入工程で挿入された前記暗号化された第１の情報を、前記秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した前記第１の情報を受信する復号化工程と、

前記プロトコルに基づいて前記基地局装置側から前記無線端末側に対して送信されるパケットに、前記セッション共有鍵の生成に用いる第２の情報を挿入する第２挿入工程と、

前記基地局装置側で、前記復号化工程で復号化された前記第１の情報に基づいて前記セッション共有鍵を生成する第１生成工程と、

前記無線端末側で、前記第２挿入工程で挿入された前記第２の情報に基づいて前記セッション共有鍵を生成する第２生成工程と、

を含むことを特徴とする無線端末認証方法。

【請求項７】　前記プロトコルは、ネットワーク層アドレスとＭＡＣアドレスとを対応させるプロトコルであることを特徴とする請求項６に記載の無線端末認証方法。

【請求項８】　前記プロトコルは、ＡＲＰであることを特徴とする請求項６に記載の無線端末認証方法。

【請求項９】　前記プロトコルは、ネットワーク層アドレスを前記無線端末に割り当てるプロトコルであることを特徴とする請求項６に記載の無線端末認証方法。

【請求項１０】　前記プロトコルは、ＤＨＣＰであることを特徴とする請求項６に記載の無線端末認証方法。

【請求項１１】　前記第１の情報および前記第２の情報は、ディフィーヘルマン型公開鍵配送法の公開鍵であり、

前記セッション共有鍵は、ディフィーヘルマン型公開鍵配送法の共有鍵であることを特徴とする請求項６～１０のいずれか一つに記載の無線端末認証方法。

【請求項１２】　さらに、前記無線端末側から前記基地局装置側に対して送信されるパケットのデータリンク層ペイロードおよび前記第２生成工程で生成された前記セッション共有鍵を含むデータに基づいてハッシュ値を算出する第１ハッシュ値算出工程と、

前記パケットのＭＡＣヘッダおよび前記ペイロードならびに前記第１ハッシュ値算出工程で算出された前記ハッシュ値を含むデータに基づいてＣＲＣ値を算出する第１ＣＲＣ値算出工程と、

前記第１ＣＲＣ値算出工程で算出された前記ＣＲＣ値を前記ＭＡＣヘッダおよび前記ペイロードに付加したパケットを前記無線端末側から前記基地局装置側に対して送信するパケット送信工程と、

前記基地局装置側で、前記パケット送信工程で送信された前記ペイロードおよび前記第１生成工程で生成された前記セッション共有鍵を含むデータに基づいてハッシュ値を算出する第２ハッシュ値算出工程と、

前記パケット送信工程で送信された前記ＭＡＣヘッダおよび前記ペイロードならびに前記第２ハッシュ値算出工程で算出された前記ハッシュ値を含むデータに基づいてＣＲＣ値を算出する第２ＣＲＣ値算出工程と、

前記基地局装置側で、前記パケット送信工程で送信された前記ＣＲＣ値と前記第２ＣＲＣ値算出工程で算出された前記ＣＲＣ値とを比較することによって、前記無線端末をパケット単位で認証する認証工程と、

を含むことを特徴とする請求項６～１１のいずれか一つに記載の無線端末認証方法。

【請求項１３】　パケットを中継する基地局装置と無線を介して通信する無線端末において、

前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記基地局装置側に対して送信するパケットに、秘匿用および／または認証用のセ

ッション共有鍵の生成に用いる第１の情報を挿入する挿入手段と、

前記プロトコルに基づいて前記基地局装置側から送信されるパケットに含まれる前記セッション共有鍵生成用の第２の情報を取得する取得手段と、

前記取得手段が取得した前記第２の情報に基づいて前記セッション共有鍵を生成する生成手段と、

を具備することを特徴とする無線端末。

【請求項１４】　パケットを中継する基地局装置と無線を介して通信する無線端末において、

当該無線端末の認証用のセッション共有鍵の生成に用いる第１の情報を秘密鍵によって暗号化する暗号化手段と、

前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記基地局装置側に対して送信するパケットに、前記暗号化手段が暗号化した前記第１の情報を挿入する挿入手段と、

前記プロトコルに基づいて前記基地局装置側から送信されるパケットに含まれる前記セッション共有鍵生成用の第２の情報を取得する取得手段と、

前記取得手段が取得した前記第２の情報に基づいて前記セッション共有鍵を生成する生成手段と、

を具備することを特徴とする無線端末。

【請求項１５】　さらに、前記基地局装置側に対して送信するパケットのデータリンク層ペイロードおよび前記生成手段が生成した前記セッション共有鍵を含むデータに基づいてハッシュ値を算出するハッシュ値算出手段と、

前記パケットのＭＡＣヘッダおよび前記ペイロードならびに前記ハッシュ値算出手段が算出した前記ハッシュ値を含むデータに基づいてＣＲＣ値を算出するＣＲＣ値算出手段と、

前記ＣＲＣ値算出手段が算出した前記ＣＲＣ値を前記ＭＡＣヘッダおよび前記ペイロードに付加したパケットを前記基地局装置側に対して送信するパケット送信手段と、

を具備することを特徴とする請求項１４に記載の無線端末。

【請求項１６】　無線端末が送受信するパケットを中継する基地局装置にお

いて、

前記無線端末との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から送信されるパケットに含まれ、秘匿用および／または認証用のセッション共有鍵の生成に用いる第１の情報を取得する取得手段と、

前記プロトコルに基づいて前記無線端末側に対して送信するパケットに、前記セッション共有鍵の生成に用いる第２の情報を挿入する挿入手段と、

前記取得手段が取得した前記第１の情報に基づいて前記セッション共有鍵を生成する生成手段と、

を具備することを特徴とする基地局装置。

【請求項１７】　無線端末が送受信するパケットを中継する基地局装置において、

前記無線端末との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から送信されるパケットに含まれ、秘密鍵によって暗号化された、前記無線端末の認証用のセッション共有鍵の生成に用いる第１の情報を取得する取得手段と、

前記取得手段が取得した前記暗号化された第１の情報を、前記秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した前記第１の情報を受信する復号化手段と、

前記プロトコルに基づいて前記無線端末側に対して送信するパケットに、前記セッション共有鍵の生成に用いる第２の情報を挿入する挿入手段と、

前記復号化手段が受信した前記第１の情報に基づいて前記セッション共有鍵を生成する生成手段と、

を具備することを特徴とする基地局装置。

【請求項１８】　さらに、前記無線端末側から受信したパケットのデータリンク層ペイロードおよび前記生成手段が生成した前記セッション共有鍵を含むデータに基づいてハッシュ値を算出するハッシュ値算出手段と、

前記パケットのＭＡＣヘッダおよび前記ペイロードならびに前記ハッシュ値算出手段が算出した前記ハッシュ値を含むデータに基づいてＣＲＣ値を算出するＣＲＣ値算出手段と、

前記無線端末側から受信した前記パケットのＣＲＣ値と前記ＣＲＣ値算出手段が算出した前記ＣＲＣ値とを比較することによって、前記無線端末をパケット単位で認証する認証手段と、

を具備することを特徴とする請求項１７に記載の基地局装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、同一データリンク層内部の無線端末および基地局装置が無線を介して通信する無線通信ネットワークシステムにおけるセッション共有鍵共有方法、無線端末認証方法、無線端末および基地局装置に関する。なお、同一データリンク層内部とは、ルータを介さずに通信することができる範囲内を意味する。

【０００２】

【従来の技術】

従来、ＩＥＥＥ８０２．１１として標準化された無線ＬＡＮ方式が知られている。この無線ＬＡＮ方式では、アクセス方式として、ＣＳＭＡ／ＣＡ（Carrier Sense Multiple Access with Collision Avoid）が用いられる。また、この無線ＬＡＮ方式では、通信を開始するための認証手順は特に規定されておらず、各無線端末は基本的に自由にネットワークに対するアクセスを行うことができる。

【０００３】

【発明が解決しようとする課題】

しかしながら、上述した技術によれば、不正な第３者による通信の傍受や発信が容易な無線を介して無線端末側と基地局装置側との通信を行い、秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に共有させる手順が規定されていないため、秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができないという問題点があった。

【０００４】

また、上述した技術によれば、不正な第３者による通信の傍受や発信が容易な無線を介して無線端末側と基地局装置側との通信を行い、ネットワークに接続す

る無線端末を認証するための手順が規定されていないため、ネットワークに対する不正アクセスが行われる危険性が高いという問題点があった。また、ハンドオーバの必要があるとともにパケット落ちの確率が高い無線端末による通信を行う場合、無線端末と基地局装置との通信を開始するときのパケット交換回数を増加させると、通信確立までの遅延が増大するという不具合がある。

【０００５】

この発明は上記に鑑みてなされたものであって、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることを第１の目的とする。また、この発明は上記に鑑みてなされたものであって、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することを第２の目的とする。

【０００６】

【課題を解決するための手段】

上記の目的を達成するために、請求項１に係るセッション共有鍵共有方法は、パケットを送受信する無線端末と該パケットを中継する基地局装置とが無線を介して通信する場合に、秘匿用および／または認証用のセッション共有鍵を前記無線端末側および前記基地局装置側に共有させるセッション共有鍵共有方法であって、前記無線端末と前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から前記基地局装置側に対して送信されるパケットに前記セッション共有鍵の生成に用いる第１の情報を挿入する第１挿入工程と、前記プロトコルに基づいて前記基地局装置側から前記無線端末側に対して送信されるパケットに、前記セッション共有鍵の生成に用いる第２の情報を挿入する第２挿入工程と、前記基地局装置側で、前記第１挿入工程で挿入された前記第１の情報に基づいて前記セッション共有鍵を生成する第１生成工程と、前記無線端末側で、前記第２挿入工程で挿入された前記第２の情報に基づいて前記セッション共有鍵を生成する第２生成工程と、を含むものである。

【０００７】

この請求項１のセッション共有鍵共有方法にあっては、第１挿入工程で、無線

端末と基地局装置との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から基地局装置側に対して送信されるパケットにセッション共有鍵の生成に用いる第１の情報を挿入し、第２挿入工程で、このプロトコルに基づいて基地局装置側から無線端末側に対して送信されるパケットに、セッション共有鍵の生成に用いる第２の情報を挿入し、第１生成工程で、基地局装置側で第１の情報に基づいてセッション共有鍵を生成し、第２生成工程で、無線端末側で第２の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【０００８】

また、請求項２に係るセッション共有鍵共有方法は、請求項１に記載のセッション共有鍵共有方法において、前記プロトコルが、ネットワーク層アドレスとＭＡＣアドレスとを対応させるプロトコルであるものである。

【０００９】

この請求項２のセッション共有鍵共有方法にあっては、ネットワーク層アドレスとＭＡＣアドレスとを対応させるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【００１０】

また、請求項３に係るセッション共有鍵共有方法は、請求項１に記載のセッション共有鍵共有方法において、前記プロトコルが、ＡＲＰであるものである。

【００１１】

この請求項３のセッション共有鍵共有方法にあっては、ＡＲＰに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【００１２】

また、請求項４に係るセッション共有鍵共有方法は、請求項１に記載のセッション共有鍵共有方法において、前記プロトコルが、ネットワーク層アドレスを前記無線端末に割り当てるプロトコルであるものである。

【００１３】

この請求項４のセッション共有鍵共有方法にあっては、ネットワーク層アドレスを無線端末に割り当てるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【００１４】

また、請求項５に係るセッション共有鍵共有方法は、請求項１に記載のセッション共有鍵共有方法において、前記プロトコルが、ＤＨＣＰであるものである。

【００１５】

この請求項５のセッション共有鍵共有方法にあっては、ＤＨＣＰに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【００１６】

また、請求項６に係る無線端末認証方法は、パケットを送受信する無線端末と該パケットを中継する基地局装置とが無線を介して通信する場合に、前記基地局装置側で前記無線端末を認証する無線端末認証方法であって、前記認証に用いるセッション共有鍵の生成用の第１の情報を秘密鍵によって暗号化する暗号化工程と、前記無線端末と前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から前記基地局装置側に対して送信されるパケットに、前記暗号化工程で暗号化された前記第１の情報を挿入する第１挿入工程と、前記基地局装置側で、前記第１挿入工程で挿入された前記暗号化された第１の

情報を、前記秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した前記第１の情報を受信する復号化工程と、前記プロトコルに基づいて前記基地局装置側から前記無線端末側に対して送信されるパケットに、前記セッション共有鍵の生成に用いる第２の情報を挿入する第２挿入工程と、前記基地局装置側で、前記復号化工程で復号化された前記第１の情報に基づいて前記セッション共有鍵を生成する第１生成工程と、前記無線端末側で、前記第２挿入工程で挿入された第２の情報に基づいて前記セッション共有鍵を生成する第２生成工程と、を含むものである。

【００１７】

この請求項６の無線端末認証方法にあっては、暗号化工程で、認証に用いるセッション共有鍵の生成用の第１の情報を秘密鍵によって暗号化し、第１挿入工程で、無線端末と基地局装置との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から基地局装置側に対して送信されるパケットに、暗号化工程で暗号化された第１の情報を挿入し、復号化工程で、暗号化された第１の情報を基地局から認証局に送信し、該認証局が復号化した第１の情報を基地局で受信し、第２挿入工程で、このプロトコルに基づいて基地局装置側から無線端末側に対して送信されるパケットに、セッション共有鍵の生成に用いる第２の情報を挿入し、第１生成工程で、復号化工程で復号化された第１の情報に基づいてセッション共有鍵を生成し、第２生成工程で、第２挿入工程で挿入された第２の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００１８】

また、請求項７に係る無線端末認証方法は、請求項６に記載の無線端末認証方法において、前記プロトコルが、ネットワーク層アドレスとＭＡＣアドレスとを対応させるプロトコルであるものである。

【００１９】

この請求項７の無線端末認証方法にあっては、ネットワーク層アドレスとＭＡ

Ｃアドレスとを対応させるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００２０】

また、請求項８に係る無線端末認証方法は、請求項６に記載の無線端末認証方法において、前記プロトコルが、ＡＲＰであるものである。

【００２１】

この請求項８の無線端末認証方法にあっては、ＡＲＰに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００２２】

また、請求項９に係る無線端末認証方法は、請求項６に記載の無線端末認証方法において、前記プロトコルが、ネットワーク層アドレスを前記無線端末に割り当てるプロトコルであるものである。

【００２３】

この請求項９の無線端末認証方法にあっては、ネットワーク層アドレスを無線端末に割り当てるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００２４】

また、請求項１０に係る無線端末認証方法は、請求項６に記載の無線端末認証方法において、前記プロトコルが、ＤＨＣＰであるものである。

【００２５】

この請求項１０の無線端末認証方法にあっては、ＤＨＣＰに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００２６】

また、請求項１１に係る無線端末認証方法は、請求項６～１０のいずれか一つに記載の無線端末認証方法において、前記第１の情報および前記第２の情報が、ディフィーヘルマン型公開鍵配送法の公開鍵であり、前記セッション共有鍵が、ディフィーヘルマン型公開鍵配送法の共有鍵であるものである。

【００２７】

この請求項１１の無線端末認証方法にあっては、ディフィーヘルマン型公開鍵配送法を用いてセッション共有鍵を無線端末側および基地局装置側に共有させることによって、セッション共有鍵をさらに適切に保護することができる。

【００２８】

また、請求項１２に係る無線端末認証方法は、請求項６～１１のいずれか一つに記載の無線端末認証方法において、さらに、前記無線端末側から前記基地局装置側に対して送信されるパケットのデータリンク層ペイロードおよび前記第２生成工程で生成された前記セッション共有鍵を含むデータに基づいてハッシュ値を算出する第１ハッシュ値算出工程と、前記パケットのＭＡＣヘッダおよび前記ペイロードならびに前記第１ハッシュ値算出工程で算出された前記ハッシュ値を含むデータに基づいてＣＲＣ値を算出する第１ＣＲＣ値算出工程と、前記第１ＣＲＣ値算出工程で算出された前記ＣＲＣ値を前記ＭＡＣヘッダおよび前記ペイロードに付加したパケットを前記無線端末側から前記基地局装置側に対して送信するパケット送信工程と、前記基地局装置側で、前記パケット送信工程で送信された前記ペイロードおよび前記第１生成工程で生成された前記セッション共有鍵を含むデータに基づいてハッシュ値を算出する第２ハッシュ値算出工程と、前記パケット送信工程で送信された前記ＭＡＣヘッダおよび前記ペイロードならびに前記第２ハッシュ値算出工程で算出された前記ハッシュ値を含むデータに基づいてＣ

ＲＣ値を算出する第２ＣＲＣ値算出工程と、前記基地局装置側で、前記パケット送信工程で送信された前記ＣＲＣ値と前記第２ＣＲＣ値算出工程で算出された前記ＣＲＣ値とを比較することによって、前記無線端末をパケット単位で認証する認証工程と、を含むものである。

【００２９】

この請求項１２の無線端末認証方法にあっては、第１ハッシュ値算出工程で、無線端末側から基地局装置側に対して送信されるパケットのデータリンク層ペイロードおよび第２生成工程で生成されたセッション共有鍵を含むデータに基づいてハッシュ値を算出し、第１ＣＲＣ値算出工程で、ＭＡＣヘッダおよびペイロードならびに第１ハッシュ値算出工程で算出されたハッシュ値を含むデータに基づいてＣＲＣ値を算出し、パケット送信工程で、第１ＣＲＣ値算出工程で算出されたＣＲＣ値をＭＡＣヘッダおよびペイロードに付加したパケットを無線端末側から基地局装置側に対して送信し、第２ハッシュ値算出工程で、パケット送信工程で送信されたペイロードおよび第１生成工程で生成されたセッション共有鍵を含むデータに基づいてハッシュ値を算出し、第２ＣＲＣ値算出工程で、パケット送信工程で送信されたＭＡＣヘッダおよびペイロードならびに第２ハッシュ値算出工程で算出されたハッシュ値を含むデータに基づいてＣＲＣ値を算出し、認証工程で、パケット送信工程で送信されたＣＲＣ値と第２ＣＲＣ値算出工程で算出されたＣＲＣ値とを比較することによって、基地局側で無線端末をパケット単位で認証する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができる。

【００３０】

また、請求項１３に係る無線端末は、パケットを中継する基地局装置と無線を介して通信する無線端末において、前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記基地局装置側に対して送信するパケットに、秘匿用および／または認証用のセッション共有鍵の生成に用いる第１の情報を挿入する挿入手段と、前記プロトコルに基づいて前記基地局装置側から送信されるパケットに含まれる前記セッション共有鍵生成用の第２の情報を取得する取得手段と、前記取得手段が取得した前記第２の情報に基づいて前記セッション共有鍵

を生成する生成手段と、を具備するものである。

【００３１】

この請求項１３の無線端末にあっては、挿入手段が、基地局装置との通信を開始する場合に実行されるプロトコルに基づいて基地局装置側に対して送信するパケットに、秘匿用および／または認証用のセッション共有鍵の生成に用いる第１の情報を挿入し、取得手段が、このプロトコルに基づいて基地局装置側から送信されるパケットに含まれるセッション共有鍵生成用の第２の情報を取得し、生成手段が、取得手段が取得した第２の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【００３２】

また、請求項１４に係る無線端末は、パケットを中継する基地局装置と無線を介して通信する無線端末において、当該無線端末の認証用のセッション共有鍵の生成に用いる第１の情報を秘密鍵によって暗号化する暗号化手段と、前記基地局装置との通信を開始する場合に実行されるプロトコルに基づいて前記基地局装置側に対して送信するパケットに、前記暗号化手段が暗号化した前記第１の情報を挿入する挿入手段と、前記プロトコルに基づいて前記基地局装置側から送信されるパケットに含まれる前記セッション共有鍵生成用の第２の情報を取得する取得手段と、前記取得手段が取得した前記第２の情報に基づいて前記セッション共有鍵を生成する生成手段と、を具備するものである。

【００３３】

この請求項１４の無線端末にあっては、暗号化手段が、当該無線端末の認証用のセッション共有鍵の生成に用いる第１の情報を秘密鍵によって暗号化し、挿入手段が、基地局装置との通信を開始する場合に実行されるプロトコルに基づいて基地局装置側に対して送信するパケットに、暗号化手段が暗号化した第１の情報を挿入し、取得手段が、このプロトコルに基づいて基地局装置側から送信されるパケットに含まれるセッション共有鍵生成用の第２の情報を取得し、生成手段が、取得手段が取得した第２の情報に基づいてセッション共有鍵を生成する。これ

により、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００３４】

また、請求項１５に係る無線端末は、請求項１４に記載の無線端末において、さらに、前記基地局装置側に対して送信するパケットのデータリンク層ペイロードおよび前記生成手段が生成した前記セッション共有鍵を含むデータに基づいてハッシュ値を算出するハッシュ値算出手段と、前記パケットのＭＡＣヘッダおよび前記ペイロードならびに前記ハッシュ値算出手段が算出した前記ハッシュ値を含むデータに基づいてＣＲＣ値を算出するＣＲＣ値算出手段と、前記ＣＲＣ値算出手段が算出した前記ＣＲＣ値を前記ＭＡＣヘッダおよび前記ペイロードに付加したパケットを前記基地局装置側に対して送信するパケット送信手段と、を具備するものである。

【００３５】

この請求項１５の無線端末にあっては、ハッシュ値算出手段が、基地局装置側に対して送信するパケットのペイロードおよび生成手段が生成したセッション共有鍵を含むデータに基づいてハッシュ値を算出し、ＣＲＣ値算出手段が、送信パケットのＭＡＣヘッダおよびペイロードならびにハッシュ値算出手段が算出したハッシュ値を含むデータに基づいてＣＲＣ値を算出し、パケット送信手段が、ＣＲＣ値算出手段が算出したＣＲＣ値をＭＡＣヘッダおよびペイロードに付加したパケットを基地局装置側に対して送信する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができる。

【００３６】

また、請求項１６に係る基地局装置は、無線端末が送受信するパケットを中継する基地局装置において、前記無線端末との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から送信されるパケットに含まれ、秘匿用および／または認証用のセッション共有鍵の生成に用いる第１の情報を取得する取得手段と、前記プロトコルに基づいて前記無線端末側に対して送信するパケットに、前記セッション共有鍵の生成に用いる第２の情報を挿入する挿入手段と、前

記取得手段が取得した前記第１の情報に基づいて前記セッション共有鍵を生成する生成手段と、を具備するものである。

【００３７】

この請求項１６の基地局装置にあっては、取得手段が、無線端末との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から送信されるパケットに含まれ、秘匿用および／または認証用のセッション共有鍵の生成に用いる第１の情報を取得し、挿入手段が、このプロトコルに基づいて無線端末側に対して送信するパケットに、セッション共有鍵の生成に用いる第２の情報を挿入し、生成手段が、取得手段が取得した第１の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができる。

【００３８】

また、請求項１７に係る基地局装置は、無線端末が送受信するパケットを中継する基地局装置において、前記無線端末との通信を開始する場合に実行されるプロトコルに基づいて前記無線端末側から送信されるパケットに含まれ、秘密鍵によって暗号化された、前記無線端末の認証用のセッション共有鍵の生成に用いる第１の情報を取得する取得手段と、前記取得手段が取得した前記暗号化された第１の情報を、前記秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した前記第１の情報を受信する復号化手段と、前記プロトコルに基づいて前記無線端末側に対して送信するパケットに、前記セッション共有鍵の生成に用いる第２の情報を挿入する挿入手段と、前記復号化手段が受信した前記第１の情報に基づいて前記セッション共有鍵を生成する生成手段と、を具備するものである。

【００３９】

この請求項１７の基地局装置にあっては、取得手段が、無線端末との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から送信されるパケットに含まれ、秘密鍵によって暗号化された、無線端末の認証用のセッション共有鍵の生成に用いる第１の情報を取得し、復号化手段が、取得手段が取得した暗号

化された第１の情報を、この秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した第１の情報を受信し、挿入手段が、このプロトコルに基づいて無線端末側に対して送信するパケットに、セッション共有鍵の生成に用いる第２の情報を挿入し、生成手段が、復号化手段が受信した第１の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００４０】

また、請求項１８に係る基地局装置は、請求項１７に記載の基地局装置において、さらに、前記無線端末側から受信したパケットのデータリンク層ペイロードならびに前記生成手段が生成した前記セッション共有鍵を含むデータに基づいてハッシュ値を算出するハッシュ値算出手段と、前記パケットのＭＡＣヘッダおよび前記ペイロードならびに前記ハッシュ値算出手段が算出した前記ハッシュ値を含むデータに基づいてＣＲＣ値を算出するＣＲＣ値算出手段と、前記無線端末側から受信した前記パケットのＣＲＣ値と前記ＣＲＣ値算出手段が算出した前記ＣＲＣ値とを比較することによって、前記無線端末をパケット単位で認証する認証手段と、を具備するものである。

【００４１】

この請求項１８の基地局装置にあっては、ハッシュ値算出手段が、無線端末側から受信したパケットのデータリンク層ペイロードおよび生成手段が生成したセッション共有鍵を含むデータに基づいてハッシュ値を算出し、ＣＲＣ値算出手段が、このパケットのＭＡＣヘッダおよびペイロードならびにハッシュ値算出手段が算出したハッシュ値を含むデータに基づいてＣＲＣ値を算出し、認証手段が、無線端末側から受信したパケットのＣＲＣ値とＣＲＣ値算出手段が算出したＣＲＣ値とを比較することによって、無線端末をパケット単位で認証する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができる。

【００４２】

【発明の実施の形態】

以下に、この発明の実施の形態を、添付の図面を参照して詳細に説明する。なお、この実施の形態によってこの発明が限定されるものではない。

【００４３】

図１は、この発明の一実施の形態にかかる通信ネットワークシステムの構成を示す説明図である。この通信ネットワークシステムは、バックボーンネットワーク４３と、バックボーンネットワーク４３とインターネット１とを接続するルータ２と、事業者ごとの広域ＬＡＮ１０－１～１０－Ｎ１と、各広域ＬＡＮ１０－１～１０－Ｎ１をバックボーンネットワーク４３にそれぞれ接続するルータ３－１～３－Ｎ１とを備える。各広域ＬＡＮ１０－１～１０－Ｎ１には、少なくとも一つの基地局（アクセスポイント）がそれぞれ接続されている。この例では、広域ＬＡＮ１０－１には、アクセスポイント４－１～４－Ｎ２が接続され、広域ＬＡＮ１０－Ｎ１には、アクセスポイント６－１～６－Ｎ３が接続されている。

【００４４】

各アクセスポイントは、無線端末と無線を介して接続され、無線ネットワークを形成する。この例では、アクセスポイント４－１は、無線端末８－１～８－ｋ１と接続され、無線ネットワーク４１－１を形成している。また、アクセスポイント４－Ｎ２は、無線端末８－ｋ２～８－Ｎ４と接続され、無線ネットワーク４１－Ｎ２を形成している。また、アクセスポイント６－１は、無線端末９－１～９－ｋ３と接続され、無線ネットワーク４２－１を形成している。また、アクセスポイント６－Ｎ３は、無線端末９－ｋ４～９－Ｎ５と接続され、無線ネットワーク４２－Ｎ３を形成している。各無線端末は、アクセスポイントを介してインターネット１や他の無線端末との通信を行うことができる。

【００４５】

また、各広域ＬＡＮ１０－１～１０－Ｎ１には、無線端末の認証データを保持する認証サーバ５－１～５－Ｎ１がそれぞれ接続されている。認証サーバ５－１～５－Ｎ１は、各アクセスポイントと信頼性のある通信を行うことができる。各無線端末のユーザは、いずれかの事業者と、その事業者のネットワークを利用する契約を交わしている。各認証サーバ５－１～５－Ｎ１は、自認証サーバを有す

る事業者（以下、自事業者と呼ぶ）と契約したユーザ（以下、契約ユーザと呼ぶ）の無線端末を認証する認証データを保持している。ここで、認証データとは、ユーザのＩＤおよびユーザと共有する秘密鍵である。

【００４６】

なお、鍵とは、情報を暗号化および／または復号化する情報のことである。また、ルータ２および３－１～３－Ｎ１に代えてブリッジを用いてもよい。また、各認証サーバ５－１～５－Ｎ１は、各広域ＬＡＮ１０－１～１０－Ｎ１に直接接続されていなくてもよく、たとえば、インターネット１等に接続され、各ルータ３－１～３－Ｎ１を介して各広域ＬＡＮ１０－１～１０－Ｎ１に接続されるようにしてもよい。

【００４７】

つぎに、無線端末の構成について説明する。図２は、図１に示した無線端末８－１の概略構成を示すブロック図である。無線端末８－１は、ユーザのＩＤおよび秘密鍵ならびにディフィーヘルマン型公開鍵配送法に用いる素数ｐおよび原始根αの情報を保持する記憶装置１１と、ディフィーヘルマン型公開鍵配送法に基づいて、素数ｐおよび原始根αを用いて公開鍵Y_Aを生成し、アクセスポイントからの公開鍵Y_Bを取得し、セッション共有鍵Ｋを算出して記憶装置１１に格納するディフィーヘルマン計算部１３と、ディフィーヘルマン計算部１３が生成した公開鍵Y_Aを秘密鍵で暗号化する暗号化部１５とを備える。

【００４８】

また、無線端末８－１は、アクセスポイントとの通信を開始する場合、ＤＨＣＰ（Dynamic Host Configuration Protocol）に基づくパケットの送受信を行うＤＨＣＰ処理部１６と、送信するパケットのデータリンク層ペイロードおよびセッション共有鍵Ｋを含むデータに基づいてハッシュ値を算出するハッシュ値計算部１２と、送信するパケットのデータリンク層ペイロードおよびＭＡＣアドレスならびにハッシュ値計算部１２が算出したハッシュ値を含むデータに基づいてＣＲＣ値を算出するＣＲＣ値計算部１４と、ＭＡＣフレームの送受信処理を行うパケット処理部１７と、無線を介してアクセスポイントと通信する無線通信部１８とを備える。

【００４９】

素数ｐおよび原始根αは、あらかじめ、各無線端末と各アクセスポイントとで共有されている。たとえば、原始根αとして「２」を用い、素数ｐとして７６８ビットや１０２４ビットの素数を用いる。記憶装置１１は、ＥＥＰＲＯＭや電源バックアップされたＲＡＭ等の書き込み可能な不揮発性記録媒体を有し、ＩＤ，秘密鍵，素数ｐおよび原始根αの情報を保持する。ディフィーヘルマン計算部１３は、ディフィーヘルマン型公開鍵配送法に基づいて、［０，ｐ－１］の間の整数X_Aをランダムに選び、記憶装置１１に保持された素数ｐおよび原始根αの情報ならびに整数X_Aを用いて公開鍵Y_Aを生成し、アクセスポイントからの公開鍵Y_Bを取得し、整数X_Aおよび公開鍵Y_Bを用いてセッション共有鍵Ｋを算出し、記憶装置１１に格納する。

【００５０】

暗号化部１５は、ディフィーヘルマン計算部１３が生成した公開鍵Y_Aを、記憶装置１１に保持された秘密鍵で暗号化する。ＤＨＣＰ処理部１６は、ＤＨＣＰに基づいて送信するＤＨＣＰ－ＤＩＳＣＯＶＥＲやＤＨＣＰ－ＲＥＱＵＥＳＴ等の所定のパケットに、記憶装置１１に記憶されたＩＤおよび暗号化部１５が暗号化した公開鍵Y_A（以下、暗号化された公開鍵Y_AをＥ（Y_A）と記す）を挿入する。この挿入は、パケットのＭＡＣヘッダ部分に行ってもよいし、データリンク層ペイロード部分に行ってもよい。また、ＤＨＣＰ処理部１６は、アクセスポイントからＤＨＣＰに基づいて送信されるＤＨＣＰ－ＯＦＦＥＲやＤＨＣＰ－ＡＣＫ等の所定のパケットを取得し、このパケットに含まれる公開鍵Y_Bを抽出してディフィーヘルマン計算部１３に出力する。

【００５１】

ハッシュ値計算部１２は、送信するパケットのデータリンク層ペイロードおよび記憶装置１１に保持されたセッション共有鍵Ｋを含むデータに基づいてハッシュ値を算出する。ＣＲＣ値計算部１４は、送信するパケットのデータリンク層ペイロードおよびＭＡＣアドレスならびにハッシュ値計算部１２が算出したハッシュ値を含むデータに基づいてＣＲＣ値を算出する。パケット処理部１７は、データリンク層ペイロードおよびＭＡＣアドレスならびにＣＲＣ値計算部１４が算出

したＣＲＣ値からＭＡＣフレームを生成して送信し、また、アクセスポイントからのＭＡＣフレームを受信する。

【００５２】

無線通信部１８は、無線を介してアクセスポイントと通信する。無線端末８－１は、そのユーザと契約している事業者のアクセスポイント４－１～４－Ｎ２にアクセスすることができるとともに、ローミングによって、アクセスポイント６－１～６－Ｎ３等の他の事業者のアクセスポイントに対するアクセスを行うことができる。ローミングの場合、アクセス先のネットワークの認証サーバから認証サーバ５－１に対してＥ（Y_A）およびＩＤが送信され、認証サーバ５－１は、復号化した公開鍵Y_Aを返信する。他の各無線端末も無線端末８－１と同じ構成を有する。

【００５３】

つぎに、アクセスポイントについて説明する。図３は、図１に示したアクセスポイント４－１の概略構成を示すブロック図である。アクセスポイント４－１は、広域ＬＡＮ１０－１との通信を行うＬＡＮ通信部２１と、素数ｐ，原始根α，認証サーバのアドレスおよびＤＨＣＰサーバのアドレスの情報を保持する記憶装置２２と、ディフィーヘルマン型公開鍵配送法に基づいて、無線端末からの公開鍵Y_Aを取得し、素数ｐおよび原始根αを用いて公開鍵Y_Bを生成し、セッション共有鍵Ｋを算出して記憶装置２２に格納するディフィーヘルマン計算部２４とを備える。

【００５４】

また、アクセスポイント４－１は、ＤＨＣＰに基づく所定のパケットを検出し、ディフィーヘルマン型公開鍵配送法の公開鍵の抽出および挿入を行うＤＨＣＰ処理部２３と、無線端末からのパケットのデータリンク層ペイロードおよびセッション共有鍵Ｋを含むデータに基づいてハッシュ値を算出し、このパケットのデータリンク層ペイロードおよびＭＡＣアドレスならびに算出したハッシュ値を含むデータに基づいてＣＲＣ値を算出するハッシュ値／ＣＲＣ値計算部２６と、ＭＡＣフレームの送受信処理を行うとともに無線端末のパケットごとの認証を行うパケット処理部２５と、無線を介して無線端末と通信する無線通信部２７とを備

える。

【００５５】

ＬＡＮ通信部２１は、広域ＬＡＮ１０－１との通信を行う。記憶装置２２は、ハードディスクやＲＡＭ等の記録媒体を有し、素数ｐ，原始根α，認証サーバのアドレスおよびＤＨＣＰサーバのアドレスの情報を保持する。ディフィーヘルマン計算部２４は、ディフィーヘルマン型公開鍵配送法に基づいて、無線端末からの公開鍵Y_Aを取得し、［０，ｐ－１］の間の整数X_Bをランダムに選び、記憶装置２２に保持された素数ｐおよび原始根αならびに整数X_Bを用いて公開鍵Y_Bを生成し、整数X_Bおよび公開鍵Y_Aを用いてセッション共有鍵Ｋを算出して記憶装置２２に格納する。

【００５６】

ＤＨＣＰ処理部２３は、パケット処理部２５からのパケットをＬＡＮ通信部２１に転送するとともにＬＡＮ通信部２１からのパケットをパケット処理部２５に転送する。そして、ＤＨＣＰ処理部２３は、パケット処理部２５からＬＡＮ通信部２１に転送するパケットをチェックして、Ｅ（Y_A）およびＩＤの情報を含むＤＨＣＰに基づく所定のパケットを検出し、このパケットに含まれるＥ（Y_A）およびＩＤを抽出し、認証サーバ５－１に送信して復号化を依頼し、認証サーバ５－１からの復号化された公開鍵Y_Aを受信する。

【００５７】

また、ＤＨＣＰ処理部２３は、ＬＡＮ通信部２１からパケット処理部２５に転送するパケットをチェックして、ＤＨＣＰに基づく所定のパケットを検出し、このパケットに、ディフィーヘルマン計算部２４が算出した公開鍵Y_Bを挿入してパケット処理部２５に転送する。ハッシュ値／ＣＲＣ値計算部２６は、無線端末からのパケットのデータリンク層ペイロードおよび記憶装置２２に保持されセッション共有鍵Ｋを含むデータに基づいてハッシュ値を算出し、このパケットのデータリンク層ペイロードおよびＭＡＣアドレスならびに算出したハッシュ値を含むデータに基づいてＣＲＣ値を算出する。

【００５８】

パケット処理部２５は、ＭＡＣフレームの送受信処理を行うとともに、内蔵す

る認証部２８によってパケットごとの無線端末の認証を行う。認証部２８は、無線端末からのパケットのＣＲＣ値とハッシュ値／ＣＲＣ値計算部２６が算出したＣＲＣ値とを比較し、一致するか否かに基づいて正当なアクセスであるか不正なアクセスであるかを判定し、不当なアクセスである場合は、そのパケットを破棄する。あるいは、通信の乱れによるデータエラーを考慮して、パケットの再送要求を行ってもよい。無線通信部２７は、無線を介して各無線端末と通信する。

【００５９】

なお、ここでは、認証サーバ５－１がＤＨＣＰサーバを兼ねる例を示すので、記憶装置２２には、認証サーバ５－１のアドレスの情報とＤＨＣＰサーバのアドレスの情報をまとめて保持する。また、ＤＨＣＰ処理部２３が、認証サーバ５－１宛てのＤＨＣＰに基づく所定のパケットをそのまま転送し、認証サーバ５－１が、このパケットからＥ（Y_A）およびＩＤを抽出し、復号化した公開鍵Y_AをＤＨＣＰに基づく所定のパケットとともにアクセスポイント４－１に送信してもよい。他のアクセスポイントもアクセスポイント４－１と同じ構成を有する。

【００６０】

つぎに、認証サーバについて説明する。図４は、図１に示した認証サーバ５－１の概略構成を示すブロック図である。認証サーバ５－１は、自事業者の各契約ユーザの秘密鍵およびＩＤの情報およびＤＨＣＰ用のデータを保持する記憶装置３１と、アクセスポイントによって送信されてきたＩＤに応じた秘密鍵でアクセスポイントによって送信されてきたＥ（Y_A）を復号化して返信する復号化部３２と、ＤＨＣＰの送受信処理を行うＤＨＣＰ処理部３３と、広域ＬＡＮ１０－１との通信を行うＬＡＮ通信部３４とを備える。

【００６１】

記憶装置３１は、ハードディスクやＲＡＭ等の記録媒体を有し、自事業者の各契約ユーザの秘密鍵およびＩＤの情報およびＤＨＣＰ用のデータを保持する。復号化部３２は、アクセスポイントによって送信されてきたＩＤに応じた秘密鍵でアクセスポイントによって送信されてきたＥ（Y_A）を復号化し、送信元のアクセスポイントに返信する。また、アクセスポイントによって送信されてきたＩＤが他の事業者のＩＤであって、ローミングが可能な場合は、該他の事業者の認証

サーバに該ＩＤおよびＥ（Y_A）を送信して復号化を依頼する。

【００６２】

このように、Ｅ（Y_A）の復号化は、公開鍵Y_Aを暗号化したユーザと契約した事業者の認証サーバのみによって行われるため、他の事業者が有するローミング先の認証サーバや、情報が盗難される危険性の高いアクセスポイントに秘密鍵を渡す必要がない。すなわち、秘密鍵を適切に保護することができる。ＤＨＣＰ処理部３３は、ＤＨＣＰ－ＤＩＳＣＯＶＥＲやＤＨＣＰ－ＲＥＱＵＥＳＴ等のパケットを受信し、ＤＨＣＰ－ＯＦＦＥＲやＤＨＣＰ－ＡＣＫ等のパケットを送信して、ＩＰアドレスを無線端末に動的に割り当てるＤＨＣＰ処理を行う。ＬＡＮ通信部３４は、広域ＬＡＮ１０－１との通信を行う。

【００６３】

なお、ここでは、認証サーバ５－１がＤＨＣＰサーバを兼ねる例を示したが、認証サーバ５－１とは別にＤＨＣＰサーバを設けてもよい。また、各アクセスポイント４－１～４－Ｎ２がＤＨＣＰサーバを兼ねてもよい。この場合は、各アクセスポイント４－１～４－Ｎ２のＤＨＣＰ処理部２３が、認証サーバ５－１が実行していたＤＨＣＰ処理を実行する。他の認証サーバ５－２～５－Ｎ１も認証サーバ５－１と同じ構成を有する。

【００６４】

また、前述した無線端末，アクセスポイントおよび認証サーバの各構成要素は、機能概念的なものであり、必ずしも物理的に図示したように構成されていなくてもよい。たとえば、これら各構成要素が備える処理機能のうち全部または一部を、図示しないＣＰＵ（Central Processing Unit）およびこのＣＰＵにて解釈実行されるプログラムによって実現することができる。すなわち、図示しないＲＯＭには、ＯＳ（Operating System）等と協働してＣＰＵに命令を与え、ＣＰＵに各種処理を行わせるコンピュータプログラムが格納されている。そして、ＣＰＵは、このプログラムに従って各種処理を行う。また、これら各構成要素が備える処理機能のうち全部または一部を、ワイヤードロジックによるハードウェアとして実現することも可能である。

【００６５】

つぎに、この実施の形態の動作について図５～図９を参照して説明する。図５は、この実施の形態にかかる、通信に先立ってセッション共有鍵Ｋを生成するセッション共有鍵生成処理の処理手順を示す説明図である。ここでは、無線端末８－１およびアクセスポイント４－１がセッション共有鍵Ｋを生成する場合を例に挙げる。このセッション共有鍵生成処理では、まず、無線端末８－１が、整数X_Aを決定して記憶する（Ｓ１）。つぎに、無線端末８－１は、素数ｐ，原始根αおよび整数X_Aに基づいて、式１で示される公開鍵Y_Aを算出する（Ｓ２）。

$$Y_A=\alpha\hat{}(X_A) \mod (p) \quad \cdots (式1)$$

ただし、Ａ ｍｏｄ（Ｂ）は、整数Ａを整数Ｂによって除算した余りを示し、Ａ＾（Ｂ）は、ＡのＢ乗を示す。

【００６６】

つぎに、無線端末８－１は、算出した公開鍵Y_Aを秘密鍵によって暗号化してＥ（Y_A）を生成し（Ｓ３）、ＩＤおよびＥ（Y_A）をＤＨＣＰ－ＲＥＱＵＥＳＴに挿入してアクセスポイント４－１に送信する（Ｓ４）。アクセスポイント４－１は、ＤＨＣＰ－ＲＥＱＵＥＳＴを受信すると、このＤＨＣＰ－ＲＥＱＵＥＳＴを転送するとともに、このＤＨＣＰ－ＲＥＱＵＥＳＴに含まれるＩＤおよびＥ（Y_A）を抽出し、このＩＤおよびＥ（Y_A）を認証サーバ５－１に送信してＥ（Y_A）の復号化を依頼する（Ｓ５）。認証サーバ５－１は、ＤＨＣＰ－ＲＥＱＵＥＳＴならびにＩＤおよびＥ（Y_A）を受信すると、このＩＤに対応する秘密鍵によってＥ（Y_A）を復号化し、復号化した公開鍵Y_Aを、ＤＨＣＰ－ＡＣＫとともにアクセスポイント４－１に返信する（Ｓ６）。

【００６７】

アクセスポイント４－１は、ＤＨＣＰ－ＡＣＫおよび公開鍵Y_Aを受信すると、整数X_Bを決定する（Ｓ７）。つぎに、アクセスポイント４－１は、素数ｐ，原始根αおよび整数X_Bに基づいて、式２で示される公開鍵Y_Bを算出する（Ｓ８）。

$$Y_B=\alpha\hat{}(X_B) \mod (p) \quad \cdots (式2)$$

つぎに、アクセスポイント４－１は、公開鍵Y_BをＤＨＣＰ－ＡＣＫに挿入して無線端末８－１に送信する（Ｓ９）。また、アクセスポイント４－１は、公開

鍵Y_Aおよび整数X_Bに基づいて、式３で示されるセッション共有鍵Ｋを算出して記憶する（Ｓ１０）。

【００６８】

$$K = Y_A \hat{} (X_B) \mod (p) = \alpha \hat{} (X_A \cdot X_B) \mod (p) \quad \cdots (式3)$$

一方、無線端末８－１は、ＤＨＣＰ－ＡＣＫを受信すると、ＤＨＣＰ－ＡＣＫに含まれる公開鍵Y_Bを抽出する。そして、無線端末８－１は、公開鍵Y_Bおよび整数X_Aに基づいて、式４で示されるセッション共有鍵Ｋを算出して記憶する（Ｓ１１）。

$$K = Y_B \hat{} (X_A) \mod (p) = \alpha \hat{} (X_A \cdot X_B) \mod (p) \quad \cdots (式4)$$

【００６９】

ここで、アクセスポイント４－１と無線端末８－１とが正しくセッション共有鍵Ｋを共有できた場合は、無線端末８－１と認証サーバ５－１とが秘密鍵を共有しているということがいえるので、アクセスポイント４－１は、無線端末８－１が正当な無線端末であることを認証することができる。逆に、アクセスポイント４－１と無線端末８－１とが正しくセッション共有鍵Ｋを共有できなかった場合は、無線端末８－１と認証サーバ５－１とが秘密鍵を共有していないということがいえるので、アクセスポイント４－１は、無線端末８－１が不正な無線端末であると判断することができる。

【００７０】

このように、セッション共有鍵Ｋを生成するための公開鍵Y_A，Y_Bの交換とＤＨＣＰとを複合させることによって、パケットの交換回数を増加させずにセッション共有鍵Ｋの共有を行うことができ、効率的な通信を行うことができる。また、無線端末８－１による通信を開始する場合、ハンドオーバを行う場合、および通信が途切れて通信開始時の処理を再び行う場合に、通信確立までの遅延時間の増加を防ぐことができる。無線端末８－１およびアクセスポイント４－１で共有したセッション共有鍵Ｋは、無線端末８－１とアクセスポイント４－１との間の通信において、種々の秘匿および／または認証に使用することができる。なお、

この例では、ハンドオーバのたびにセッション共有鍵を生成するが、ハンドオーバ先のアクセスポイントが元のアクセスポイントから無線端末のＩＰやセッション共有鍵を取得するようにしてもよい。

【００７１】

つぎに、ローミングを行う場合について説明する。図６は、この実施の形態にかかる、ローミングを行う場合のセッション共有鍵生成処理の処理手順を示す説明図である。ここでは、無線端末９－１およびアクセスポイント４－１がセッション共有鍵Ｋを生成する場合を例に挙げる。なお、ローミングを行わない場合と同一処理の部分については図５と同一の符号を付している。このセッション共有鍵生成処理では、認証サーバ５－１が、ステップＳ５で受信したＩＤが自事業者のＩＤでないと判定し、このＩＤに対応する事業者の認証サーバ５－Ｎ１に、このＩＤおよびＥ（Y_A）を送信してＥ（Y_A）の復号化を依頼する（Ｓ２１）。

【００７２】

認証サーバ５－Ｎ１は、認証サーバ５－１からのＩＤおよびＥ（Y_A）を受信すると、このＩＤに対応する秘密鍵によってＥ（Y_A）を復号化し、復号化した公開鍵Y_Aを認証サーバ５－１に返信する（Ｓ２２）。認証サーバ５－１は、認証サーバ５－Ｎ１からの公開鍵Y_Aを受信してアクセスポイント４－１に転送する。あるいは、認証サーバ５－Ｎ１からアクセスポイント４－１宛てに公開鍵Y_Aを送信してもよい。このように、ローミングを行う場合においても、アクセスポイント４－１および認証サーバ５－１に秘密鍵を知られることなくセッション共有鍵Ｋの共有を行うことができる。

【００７３】

つぎに、ＤＨＣＰやセッション共有鍵生成処理が終了したあとの、アクセスポイントにおける無線端末の認証処理について説明する。この認証処理では、セッション共有鍵Ｋを使ってハッシュ値を発生させ、このハッシュ値をＭＡＣフレームのＣＲＣ値に加味することによってパケット単位の認証を行う。図７は、この実施の形態にかかる無線端末のＭＡＣフレーム生成処理の処理手順を示す説明図である。このＭＡＣフレーム生成処理において、無線端末は、まず、送信パケットのデータリンク層ペイロードおよびセッション共有鍵Ｋを含むデータを生成す

る（Ｓ３１）。

【００７４】

この例では、データリンク層ペイロードをセッション共有鍵Ｋで挟んだデータを作成するが、データリンク層ペイロードとセッション共有鍵Ｋの並べ方は特に限定されず、データリンク層ペイロードの片方にセッション共有鍵Ｋを付加してもよいし、セッション共有鍵Ｋをデータリンク層ペイロードで挟んでもよい。また、セッション共有鍵Ｋおよびデータリンク層ペイロードの一部のみを用いてもよい。さらに、このデータにＭＡＣヘッダを含めてもよい。つぎに、無線端末は、ステップＳ３１で生成したデータからハッシュ値を算出する（Ｓ３２）。

【００７５】

つぎに、無線端末は、算出したハッシュ値ならびに送信パケットのＭＡＣヘッダおよびデータリンク層ペイロードを含むデータを生成する（Ｓ３３）。このデータの並べ方も特に限定されない。そして、無線端末は、ステップＳ３３で生成したデータのＣＲＣ値を算出し（Ｓ３４）、このＣＲＣ値をＭＡＣフレームのＣＲＣ値として用い（Ｓ３５）、このＭＡＣフレームをアクセスポイントに送信する。

【００７６】

図８は、この実施の形態にかかるアクセスポイントによるパケット単位の認証処理の処理手順を示す説明図である。この認証処理において、アクセスポイントは、まず、無線端末から受信したパケットのデータリンク層ペイロードおよびセッション共有鍵Ｋを含むデータを、前述した無線端末と同じ方法で生成する（Ｓ４１）。つぎに、アクセスポイントは、このデータからハッシュ値を算出する（Ｓ４２）つぎに、アクセスポイントは、算出したハッシュ値ならびに受信パケットのＭＡＣヘッダおよびデータリンク層ペイロードを含むデータを、前述した無線端末と同じ方法で生成する（Ｓ４３）。

【００７７】

そして、アクセスポイントは、ステップＳ４３で生成したデータのＣＲＣ値を算出し（Ｓ４４）、このＣＲＣ値と、受信パケットのＣＲＣ値とを比較し、これらが同一であれば、このパケットを送信した無線端末が正しいセッション共有鍵

Ｋを持つ、すなわち、その無線端末が認証サーバと共有する正しい秘密鍵を持つと判断して認証する。このように、パケットフォーマットを変更することなくパケットごとの認証を行うことができるので、データリンクの最大転送可能データ長に影響を与えることがなく、利用者にはトランスピアレントである。

【００７８】

また、この方法は、アクセスポイントから無線端末にパケットを送信する場合にも適用することができる。すなわち、アクセスポイントが前述した無線端末と同じ方法でＣＲＣ値を算出してパケットを生成し、無線端末が前述したアクセスポイントを同じ方法でＣＲＣ値を算出してパケットごとの認証を行ってもよい。これにより、無線端末側においてパケットごとの認証を行うことができ、アクセスポイントになりすました第３者からのパケットであるかアクセスポイントからの正当なパケットであるかを判定することができる。

【００７９】

つぎに、セッション共有鍵Ｋを秘匿に用いる場合について説明する。図９は、この実施の形態にかかる秘匿処理を説明する説明図である。ここでは、無線端末８－１とアクセスポイント４－１との通信を例に挙げる。この秘匿処理では、無線端末８－１がアクセスポイント４－１に対してデータパケットを送信する場合、自無線端末が有するセッション共有鍵Ｋによって該データパケットを暗号化して送信する。暗号化された暗号パケットを受信したアクセスポイント４－１は、自アクセスポイントが有するセッション共有鍵Ｋによって該暗号パケットを復号化し、宛先に送信する。

【００８０】

また、アクセスポイント４－１が無線端末８－１に対してデータパケットを送信する場合、自アクセスポイントが有するセッション共有鍵Ｋによって該データパケットを暗号化して送信する。暗号化された暗号パケットを受信した無線端末８－１は、自無線端末が有するセッション共有鍵Ｋによって該暗号パケットを復号化する。このように、不正な第３者による通信の傍受や発信が容易な無線を介するアクセスポイント４－１と無線端末９－１との通信においても、情報の秘匿を行い、適切な通信を行うことができる。

【００８１】

前述した様に、この実施の形態によれば、ＤＨＣＰに基づいて無線端末側からアクセスポイント側に対して送信されるパケットにセッション共有鍵Ｋの生成に用いる公開鍵Y_Aを挿入し、ＤＨＣＰに基づいてアクセスポイント側から無線端末側に対して送信されるパケットにセッション共有鍵Ｋの生成に用いる公開鍵Y_Bを挿入し、アクセスポイント側で公開鍵Y_Aに基づいてセッション共有鍵Ｋを生成し、無線端末側で公開鍵Y_Bに基づいてセッション共有鍵Ｋを生成する。

【００８２】

これにより、無線端末とアクセスポイントとの通信を開始する場合のパケット交換回数を増加させることなく、公開鍵Y_A，Y_Bの交換を行うことができるため、無線端末とアクセスポイントとの通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵Ｋを無線端末側およびアクセスポイント側に安全に共有させることができる。また、この実施の形態では、ＤＨＣＰを例に挙げて説明したが、ＡＲＰ（Address Resolution Protocol）等、無線端末－アクセスポイント間の通信に先立って行われる他のプロトコルを用いてもよい。この場合、前述した各ＤＨＣＰ処理部に代えて、そのプロトコルに関する処理を行う処理部を設ける。また、セッション共有鍵に代えて秘密鍵および公開鍵のペアを用いてもよい。

【００８３】

【発明の効果】

以上説明したように、この発明のセッション共有鍵共有方法（請求項１）は、第１挿入工程で、無線端末と基地局装置との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から基地局装置側に対して送信されるパケットにセッション共有鍵の生成に用いる第１の情報を挿入し、第２挿入工程で、このプロトコルに基づいて基地局装置側から無線端末側に対して送信されるパケットに、セッション共有鍵の生成に用いる第２の情報を挿入し、第１生成工程で、基地局装置側で第１の情報に基づいてセッション共有鍵を生成し、第２生成工程で、無線端末側で第２の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させる

ことなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００８４】

また、この発明のセッション共有鍵共有方法（請求項２）は、ネットワーク層アドレスとＭＡＣアドレスとを対応させるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００８５】

また、この発明のセッション共有鍵共有方法（請求項３）は、ＡＲＰに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００８６】

また、この発明のセッション共有鍵共有方法（請求項４）は、ネットワーク層アドレスを無線端末に割り当てるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全

に共有させることができる。

【００８７】

また、この発明のセッション共有鍵共有方法（請求項５）は、ＤＨＣＰに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００８８】

また、この発明の無線端末認証方法（請求項６）は、暗号化工程で、認証に用いるセッション共有鍵の生成用の第１の情報を秘密鍵によって暗号化し、第１挿入工程で、無線端末と基地局装置との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から基地局装置側に対して送信されるパケットに、暗号化工程で暗号化された第１の情報を挿入し、復号化工程で、暗号化された第１の情報を基地局から認証局に送信し、該認証局が復号化した第１の情報を基地局で受信し、第２挿入工程で、このプロトコルに基づいて基地局装置側から無線端末側に対して送信されるパケットに、セッション共有鍵の生成に用いる第２の情報を挿入し、第１生成工程で、復号化工程で復号化された第１の情報に基づいてセッション共有鍵を生成し、第２生成工程で、第２挿入工程で挿入された第２の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【００８９】

また、この発明の無線端末認証方法（請求項７）は、ネットワーク層アドレスとＭＡＣアドレスとを対応させるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交

換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【００９０】

また、この発明の無線端末認証方法（請求項８）は、ＡＲＰに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【００９１】

また、この発明の無線端末認証方法（請求項９）は、ネットワーク層アドレスを無線端末に割り当てるプロトコルに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【００９２】

また、この発明の無線端末認証方法（請求項１０）は、ＤＨＣＰに基づいて基地局装置側と無線端末側との間で送受信されるパケットにセッション共有鍵生成用の情報を挿入して交換することによって、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対す

る不正アクセスを低減することができる。

【００９３】

また、この発明の無線端末認証方法（請求項１１）は、ディフィーヘルマン型公開鍵配送法を用いてセッション共有鍵を無線端末側および基地局装置側に共有させるため、セッション共有鍵をさらに適切に保護することができる。

【００９４】

また、この発明の無線端末認証方法（請求項１２）は、第１ハッシュ値算出工程で、無線端末側から基地局装置側に対して送信されるパケットのデータリンク層ペイロードおよび第２生成工程で生成されたセッション共有鍵を含むデータに基づいてハッシュ値を算出し、第１ＣＲＣ値算出工程で、ペイロードおよび第１ハッシュ値算出工程で算出されたハッシュ値を含むデータに基づいてＣＲＣ値を算出し、パケット送信工程で、第１ＣＲＣ値算出工程で算出されたＣＲＣ値をＭＡＣヘッダおよびペイロードに付加したパケットを無線端末側から基地局装置側に対して送信し、第２ハッシュ値算出工程で、パケット送信工程で送信されたＭＡＣヘッダおよびペイロードならびに第１生成工程で生成されたセッション共有鍵を含むデータに基づいてハッシュ値を算出し、第２ＣＲＣ値算出工程で、パケット送信工程で送信されたＭＡＣヘッダおよびペイロードならびに第２ハッシュ値算出工程で算出されたハッシュ値を含むデータに基づいてＣＲＣ値を算出し、認証工程で、パケット送信工程で送信されたＣＲＣ値と第２ＣＲＣ値算出工程で算出されたＣＲＣ値とを比較することによって、基地局側で無線端末をパケット単位で認証する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができるため、さらに適切にネットワークに対する不正アクセスを低減することができる。

【００９５】

また、この発明の無線端末（請求項１３）は、挿入手段が、基地局装置との通信を開始する場合に実行されるプロトコルに基づいて基地局装置側に対して送信するパケットに、秘匿用および／または認証用のセッション共有鍵の生成に用いる第１の情報を挿入し、取得手段が、このプロトコルに基づいて基地局装置側から送信されるパケットに含まれるセッション共有鍵生成用の第２の情報を取得し

、生成手段が、取得手段が取得した第２の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００９６】

また、この発明の無線端末（請求項１４）は、暗号化手段が、当該無線端末の認証用のセッション共有鍵の生成に用いる第１の情報を秘密鍵によって暗号化し、挿入手段が、基地局装置との通信を開始する場合に実行されるプロトコルに基づいて基地局装置側に対して送信するパケットに、暗号化手段が暗号化した第１の情報を挿入し、取得手段が、このプロトコルに基づいて基地局装置側から送信されるパケットに含まれるセッション共有鍵生成用の第２の情報を取得し、生成手段が、取得手段が取得した第２の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【００９７】

また、この発明の無線端末（請求項１５）は、ハッシュ値算出手段が、基地局装置側に対して送信するパケットのペイロードおよび生成手段が生成したセッション共有鍵を含むデータに基づいてハッシュ値を算出し、ＣＲＣ値算出手段が、送信パケットのＭＡＣヘッダおよびペイロードならびにハッシュ値算出手段が算出したハッシュ値を含むデータに基づいてＣＲＣ値を算出し、パケット送信手段が、ＣＲＣ値算出手段が算出したＣＲＣ値をＭＡＣヘッダおよびペイロードに付加したパケットを基地局装置側に対して送信する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができるため、さらに適切にネットワークに対する不正アクセスを低減することができる。

【００９８】

また、この発明の基地局装置（請求項１６）は、取得手段が、無線端末との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から送信されるパケットに含まれ、秘匿用および／または認証用のセッション共有鍵の生成に用いる第１の情報を取得し、挿入手段が、このプロトコルに基づいて無線端末側に対して送信するパケットに、セッション共有鍵の生成に用いる第２の情報を挿入し、生成手段が、取得手段が取得した第１の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなくセッション共有鍵生成用の情報を交換することができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができる。

【００９９】

また、この発明の基地局装置（請求項１７）は、取得手段が、無線端末との通信を開始する場合に実行されるプロトコルに基づいて無線端末側から送信されるパケットに含まれ、秘密鍵によって暗号化された、無線端末の認証用のセッション共有鍵の生成に用いる第１の情報を取得し、復号化手段が、取得手段が取得した暗号化された第１の情報を、この秘密鍵によって暗号化された情報を復号化して返信する認証局に送信し、該認証局が復号化した第１の情報を受信し、挿入手段が、このプロトコルに基づいて無線端末側に対して送信するパケットに、セッション共有鍵の生成に用いる第２の情報を挿入し、生成手段が、復号化手段が受信した第１の情報に基づいてセッション共有鍵を生成する。これにより、無線端末と基地局装置との通信を開始する場合のパケット交換回数を増加させることなく無線端末認証用のセッション共有鍵を無線端末側および基地局装置側に安全に共有させることができるため、無線端末と基地局装置との通信確立までの遅延を抑えつつネットワークに対する不正アクセスを低減することができる。

【０１００】

また、この発明の基地局装置（請求項１８）は、ハッシュ値算出手段が、無線端末側から受信したパケットのデータリンク層ペイロードおよび生成手段が生成

したセッション共有鍵を含むデータに基づいてハッシュ値を算出し、ＣＲＣ値算出手段が、このパケットのＭＡＣヘッダおよびペイロードならびにハッシュ値算出手段が算出したハッシュ値を含むデータに基づいてＣＲＣ値を算出し、認証手段が、無線端末側から受信したパケットのＣＲＣ値とＣＲＣ値算出手段が算出したＣＲＣ値とを比較することによって、無線端末をパケット単位で認証する。これにより、パケットのフォーマットを変更することなくパケット単位の認証を行うことができるため、さらに適切にネットワークに対する不正アクセスを低減することができる。

【図面の簡単な説明】

【図１】

この発明の一実施の形態にかかる通信ネットワークシステムの構成を示す説明図である。

【図２】

図１に示した無線端末の概略構成を示すブロック図である。

【図３】

図１に示したアクセスポイントの概略構成を示すブロック図である。

【図４】

図１に示した認証サーバの概略構成を示すブロック図である。

【図５】

この実施の形態にかかるセッション共有鍵生成処理の処理手順を示す説明図である。

【図６】

この実施の形態にかかる、ローミングを行う場合のセッション共有鍵生成処理の処理手順を示す説明図である。

【図７】

この実施の形態にかかるＭＡＣフレーム生成処理の処理手順を示す説明図である。

【図８】

この実施の形態にかかる認証処理の処理手順を示す説明図である。

【図９】

この実施の形態にかかる秘匿処理を説明する説明図である。

【符号の説明】

１　インターネット

２，３－１～３－Ｎ１　ルータ

４－１～４－Ｎ２，６－１～６－Ｎ３　アクセスポイント

５－１～５－Ｎ１　認証サーバ

８－１～８－Ｎ４，９－１～９－Ｎ５　無線端末

１０－１～１０－Ｎ１　広域ＬＡＮ

１１，２２，３１　記憶装置

１２　ハッシュ値計算部

１３，２４　ディフィーヘルマン計算部

１４　ＣＲＣ値計算部

１５　暗号化部

１６，２３，３３　ＤＨＣＰ処理部

１７，２５　パケット処理部

１８，２７　無線通信部

２１，３４　ＬＡＮ通信部

２６　ハッシュ値／ＣＲＣ値計算部

２８　認証部

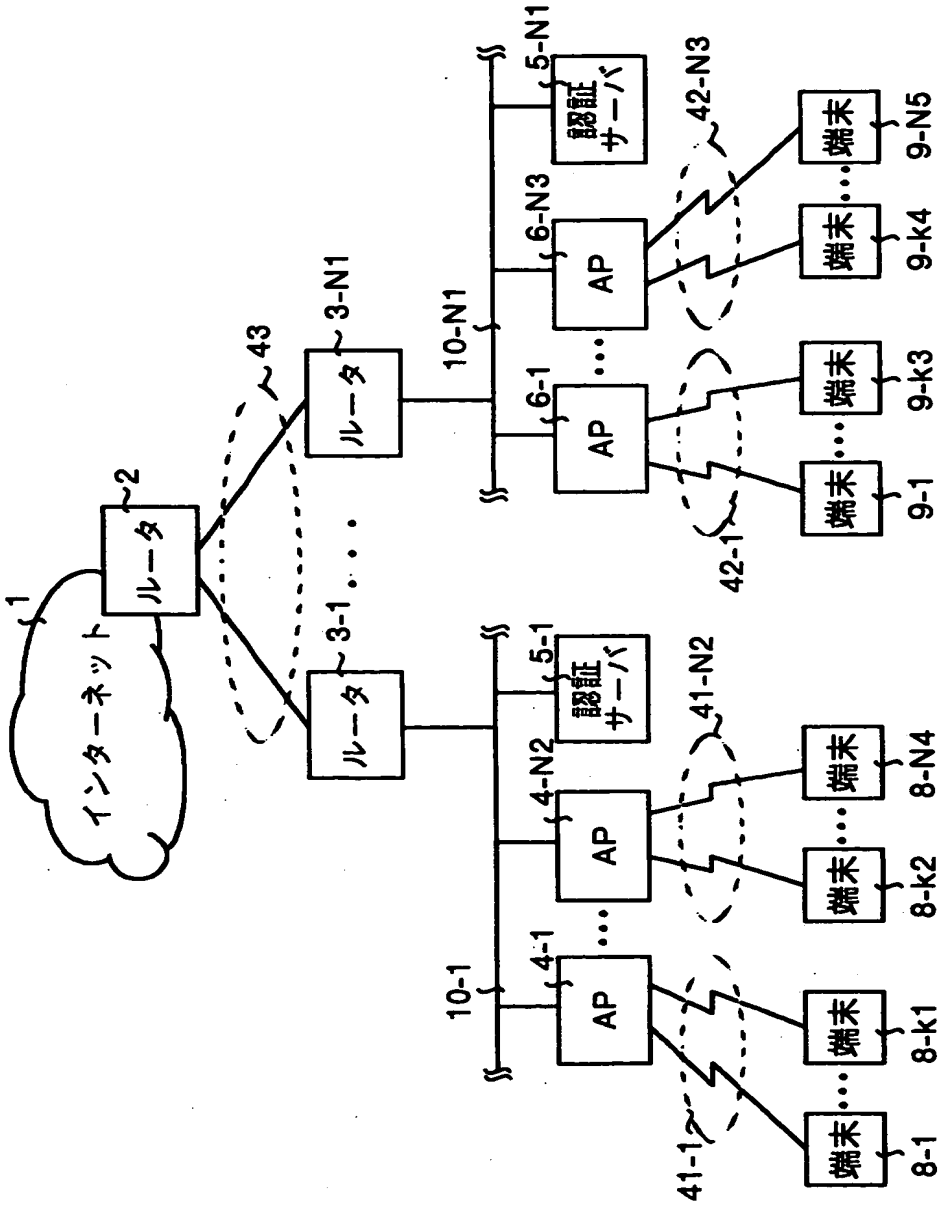
３２　復号化部

４１－１～４１－Ｎ２，４２－１～４２－Ｎ３　無線ネットワーク

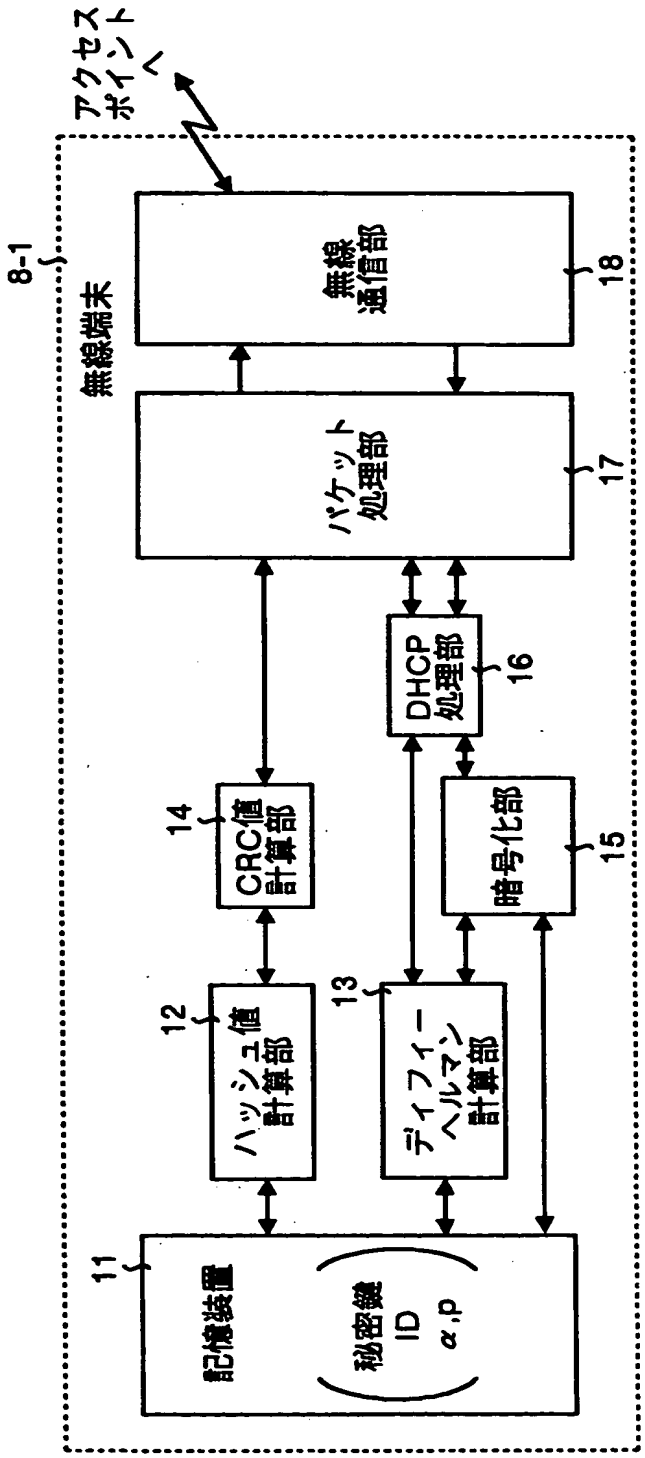
４３　バックボーンネットワーク

【書類名】　　図面

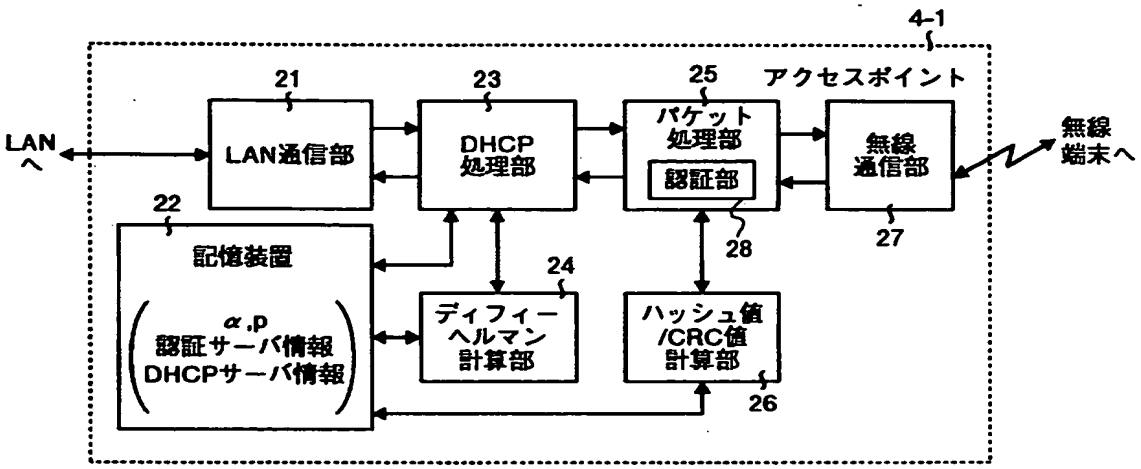
【図１】


1
インターネット
2
ルータ
43
3-1
ルータ
3-N1
ルータ
10-1
10-N1
4-1
AP
4-N2
AP
6-1
AP
6-N3
AP
5-1
認証サーバ
5-N1
認証サーバ
41-1
41-N2
42-1
42-N3
端末
8-1
8-k1
8-k2
8-N4
9-1
9-k3
9-k4
9-N5

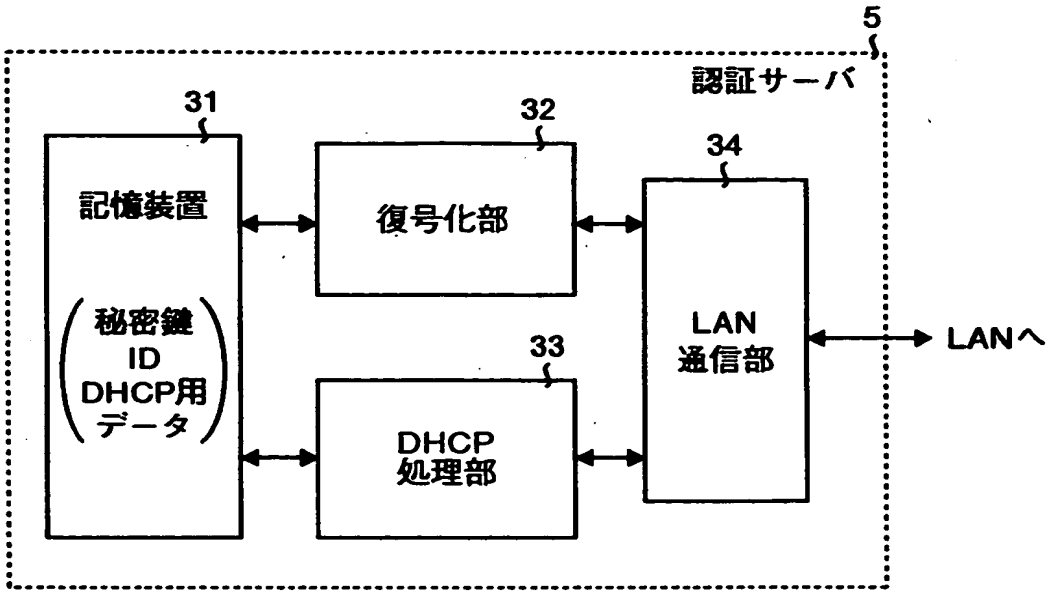
【図２】


アクセスポイント
8-1
無線端末
無線通信部
18
パケット処理部
17
DHCP処理部
16
暗号化部
15
CRC値計算部
14
ハッシュ値計算部
12
ディフィーヘルマン計算部
13
記憶装置
11
秘密鍵
ID
α,p

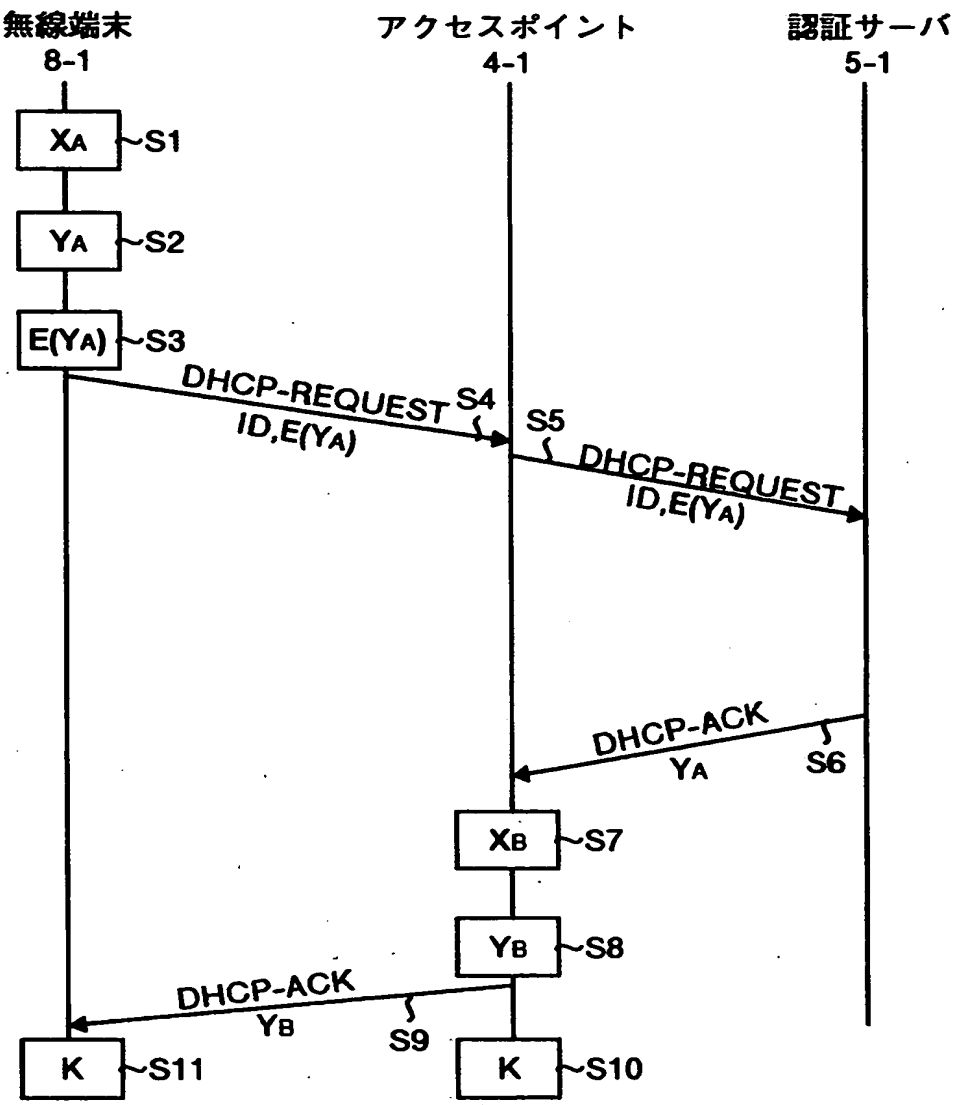
【図３】


4-1
21
23
25
アクセスポイント
LAN
へ
LAN通信部
DHCP
処理部
パケット
処理部
認証部
無線
通信部
無線
端末へ
22
記憶装置
α,p
認証サーバ情報
DHCPサーバ情報
24
ディフィー
ヘルマン
計算部
ハッシュ値
/CRC値
計算部
26
27
28

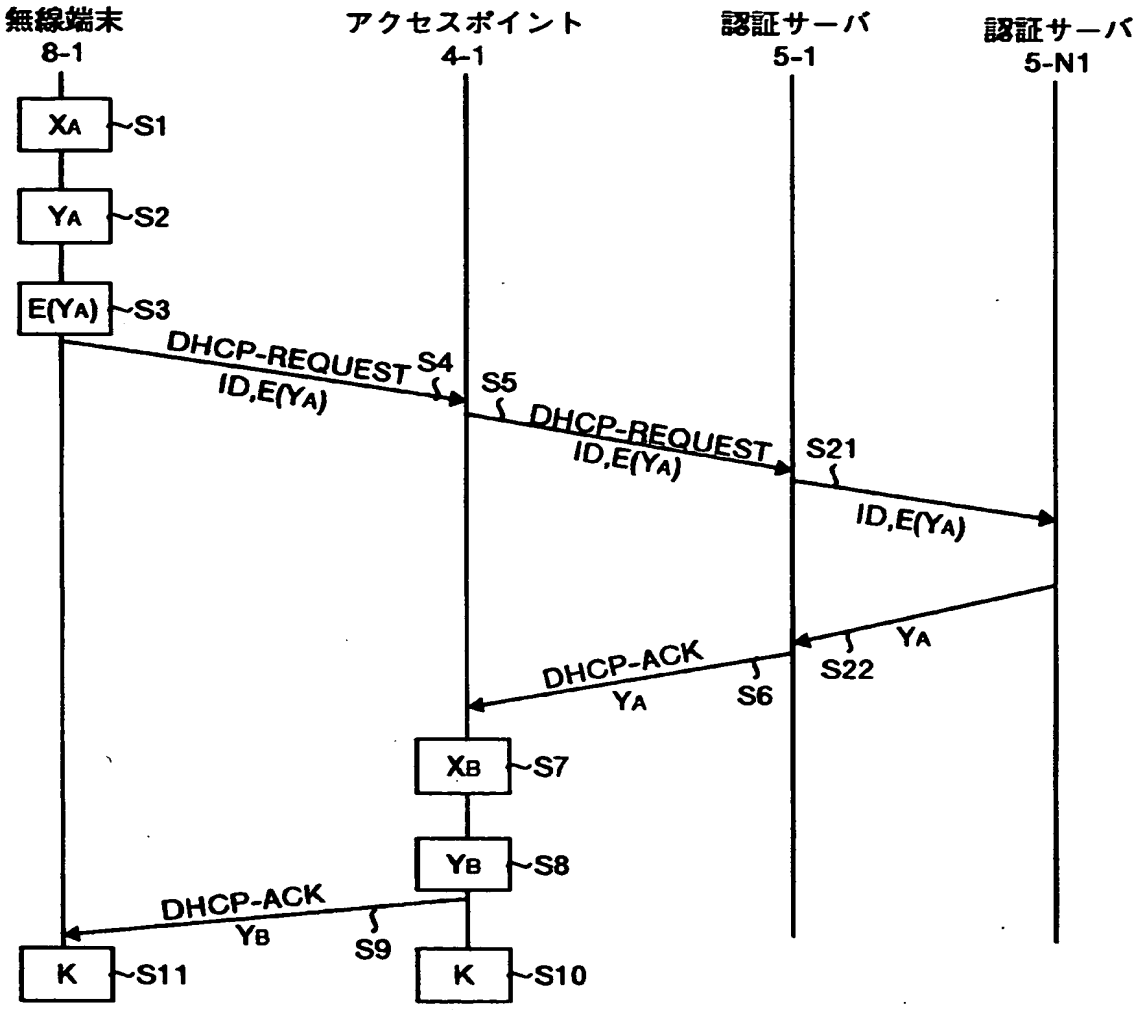
【図４】


5
認証サーバ
31
記憶装置
秘密鍵
ID
DHCP用
データ
32
復号化部
33
DHCP
処理部
34
LAN
通信部
LANへ

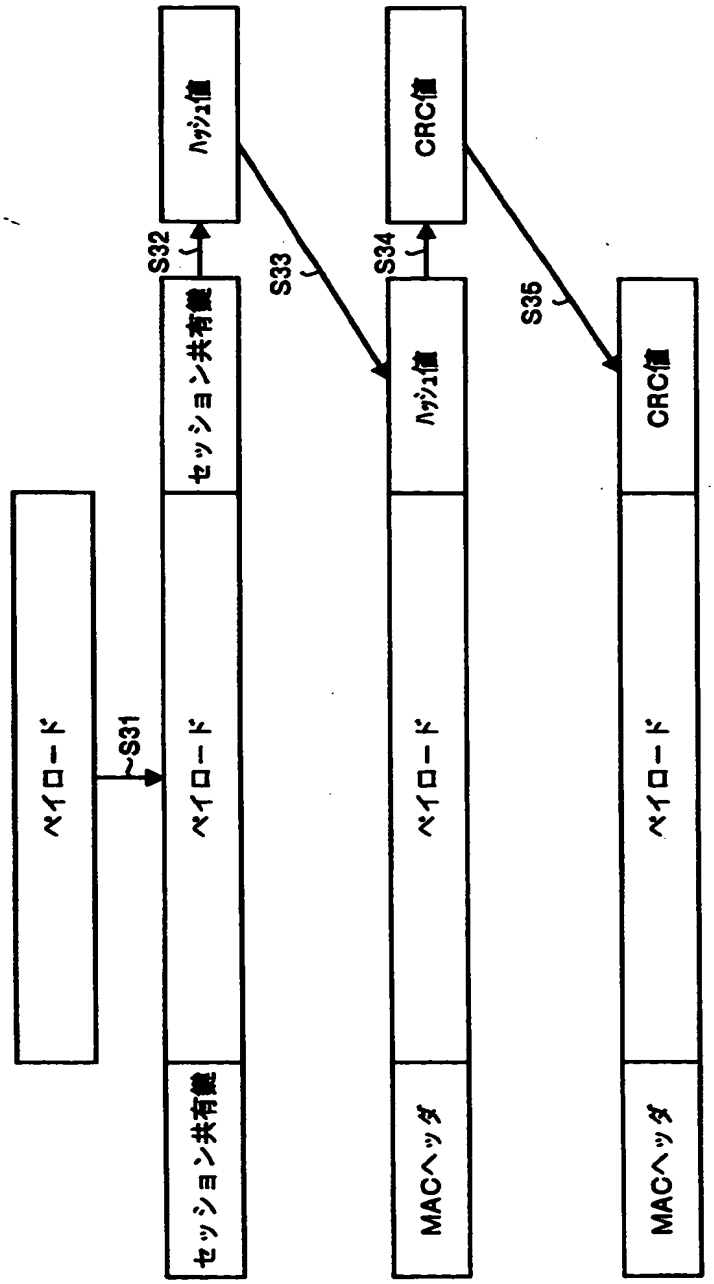
【図５】


無線端末
8-1
アクセスポイント
4-1
認証サーバ
5-1
XA
S1
YA
S2
E(YA)
S3
DHCP-REQUEST
ID,E(YA)
S4
S5
DHCP-REQUEST
ID,E(YA)
DHCP-ACK
YA
S6
XB
S7
YB
S8
DHCP-ACK
YB
S9
K
S11
K
S10

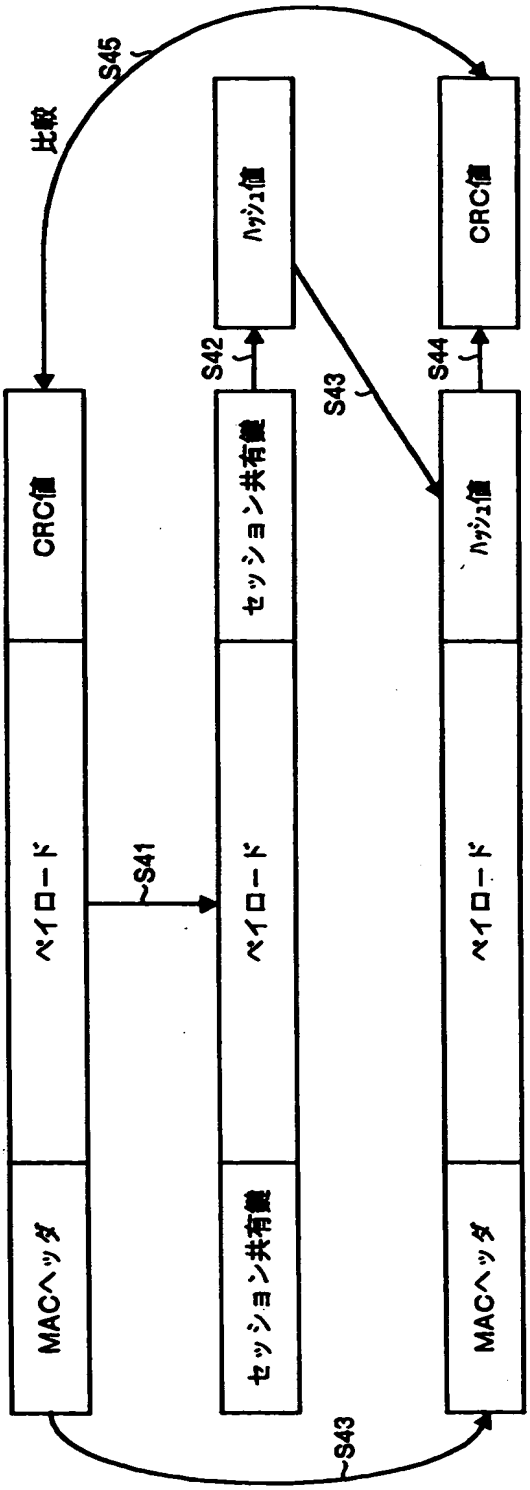
【図６】


無線端末
8-1
アクセスポイント
4-1
認証サーバ
5-1
認証サーバ
5-N1
XA
S1
YA
S2
E(YA)
S3
DHCP-REQUEST
ID,E(YA)
S4
S5
DHCP-REQUEST
ID,E(YA)
S21
ID,E(YA)
YA
S22
DHCP-ACK
YA
S6
XB
S7
YB
S8
DHCP-ACK
YB
S9
K
S11
K
S10

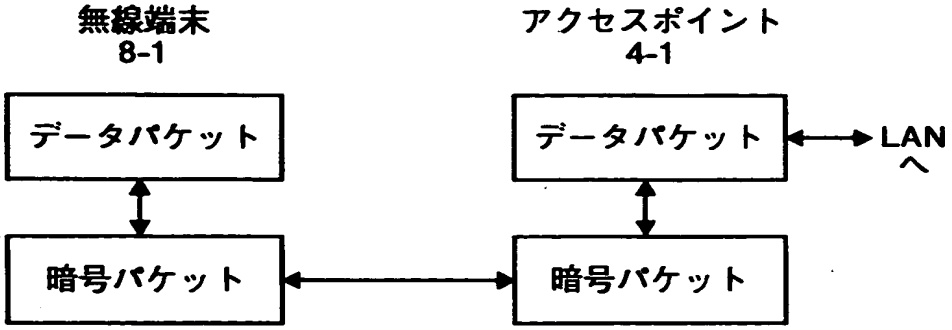
【図７】


ペイロード
S31
ペイロード
セッション共有鍵
セッション共有鍵
S32
ハッシュ値
S33
ペイロード
MACヘッダ
S34
CRC値
S35
ペイロード
MACヘッダ
CRC値

【図８】


S45
比較
ハッシュ値
CRC値
S42
S43
S44
CRC値
セッション共有鍵
ハッシュ値
ペイロード
S41
ペイロード
ペイロード
MACヘッダ
セッション共有鍵
MACヘッダ
S43

【図９】



【書類名】　　要約書

【要約】

【課題】　無線端末とアクセスポイントとの通信確立までの遅延を抑えつつ秘匿用および／または認証用のセッション共有鍵Ｋを無線端末側およびアクセスポイント側に安全に共有させること。

【解決手段】　ＤＨＣＰに基づいて無線端末８－１側からアクセスポイント４－１側に対して送信されるパケットにセッション共有鍵Ｋの生成に用いる公開鍵Y_Aを挿入し、ＤＨＣＰに基づいてアクセスポイント４－１側から無線端末８－１側に対して送信されるパケットにセッション共有鍵Ｋの生成に用いる公開鍵Y_Bを挿入し、アクセスポイント４－１側で公開鍵Y_Aに基づいてセッション共有鍵Ｋを生成し、無線端末８－１側で公開鍵Y_Bに基づいてセッション共有鍵Ｋを生成する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２９０〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目６番１号
氏　名　古河電気工業株式会社